



Microsoft Purview Information Protection and DLP: Sensitivity Labels and Auto-Labeling



Microsoft Purview Information Protection and DLP: Sensitivity Labels and Auto-Labeling

Introduction:

Microsoft Purview information protection and data loss prevention matter because sensitive files and messages leave Microsoft 365 tenants every day through forwarded mail, oversharing links, Teams chats and copies to USB drives, while nobody knows which items are confidential. Labels exist on paper but are never applied, and DLP rules either block nothing or block everything. This Core Concept course trains administrators to classify content, publish sensitivity labels, enforce DLP across mail, files, chat and devices, and retain what must be kept. Participants build an Information Protection and DLP Design for a case organisation.

Course Objectives:

- Locate sensitive content in a Microsoft 365 tenant using sensitive information types, trainable classifiers, content explorer and activity explorer
- Design and publish a sensitivity label taxonomy with label policies, visual markings, access restrictions and encryption settings
- Configure client-side and service-side auto-labelling so that labels reach documents and mail without relying on users
- Build and tune Microsoft Purview DLP policies for Exchange, SharePoint, OneDrive, Teams and Windows endpoints with policy tips, overrides and incident alerts
- Apply retention policies, retention labels and records settings, and use audit search, insider risk signals and eDiscovery cases to investigate data incidents
- Produce an Information Protection and DLP Design that maps technical controls to the organisation's data classification and privacy duties

Target Audience:

- Administrators responsible for Microsoft 365 tenant configuration across Exchange Online, SharePoint, OneDrive and Teams
 - Security and compliance administrators who build and maintain policies in the Microsoft Purview portal
 - Information protection staff who own the organisation's classification scheme and labelling rollout
 - Records and information management staff who configure retention and disposal of electronic content
 - Security operations analysts who triage DLP alerts and investigate data exposure incidents
-

Course Outline:

Day 1: Sensitive Data in the Tenant and the Purview Portal

- Data at Rest, in Motion and in Use Across Mail, Files, Chat and Devices
- Microsoft Purview Portal Tour: Solutions, Role Groups and Permissions
- Know, Protect, Prevent: The Purview Information Protection Model
- Tenant Oversharing Baseline: Sharing Links, Guest Access and Unlabelled Content
- Sensitive Data Inventory Worksheet by Business Unit and Workload

Day 2: Data Classification: Sensitive Information Types and Classifiers

- Built-In Sensitive Information Types: Patterns, Keywords, Confidence Levels and Proximity
- Custom Sensitive Information Types With Regular Expressions and Keyword Dictionaries
- Trainable Classifiers: Built-In Categories and Seed Content for Custom Models
- Content Explorer and Activity Explorer Review of Classified Items
- Classification Test Plan: False Positive and False Negative Sampling

Day 3: Sensitivity Labels, Encryption and Auto-Labelling

- Sensitivity Label Taxonomy: Parent Labels, Sublabels and Label Priority
- Label Policies: Default Label, Mandatory Labelling and Downgrade Justification
- Label Encryption, Visual Markings and Microsoft Purview Message Encryption
- Auto-Labelling Policies in Simulation Mode for SharePoint, OneDrive and Exchange
- Labels for Teams, Microsoft 365 Groups and Sites: Privacy and External Sharing Settings

Day 4: DLP Policies, Endpoints, Retention and Investigations

- DLP Policy Build: Conditions, Actions, Policy Tips and User Overrides
- Endpoint DLP on Windows Devices: USB, Printing, Cloud Upload and Browser Controls
- DLP for Teams Chats and Channels and Alert Triage in the DLP Alerts Dashboard
- Retention Policies, Retention Labels and Records Declaration for Mail and Files
- Insider Risk Signals, Audit Log Search and eDiscovery Case Basics

Day 5: Lab Build and the Information Protection and DLP Design

- Lab: Label Set With Encryption Published to a Pilot Group
 - Lab: Financial and Personal Data DLP Policy Tested in Simulation and Enforced
 - Control Mapping Matrix: Classification Levels to Labels, DLP Rules and Retention
 - Phased Rollout Plan: Pilot, User Communication and Policy Tuning Cadence
 - Information Protection and DLP Design Presentation and Peer Review
-

Skills You Will Gain:

- Sensitive Information Type Configuration
- Trainable Classifier Evaluation
- Sensitivity Label Taxonomy Design
- Auto-Labeling Policy Tuning
- Endpoint DLP Administration
- DLP Alert Triage
- Retention Label Management
- Purview Audit Investigation

Why Attend This Course:

- Leave with an Information Protection and DLP Design tested in a lab tenant and ready to adapt to your own Microsoft 365 environment
- Cut DLP noise by knowing which confidence levels, conditions and overrides stop real leaks without blocking normal work
- Know how to move labelling from optional user choice to automatic coverage of mail, files and sites
- Compare labelling and DLP rollout experience with administrators from finance, healthcare, energy and public sector organisations

Conclusion:

Protecting information in Microsoft 365 works when sensitive content is found, labelled and governed by policies that follow it across mail, files, chat and devices. The week moves from sensitive data states and the Purview portal, through sensitive information types and classifiers, to sensitivity labels, encryption and auto-labelling, then DLP for workloads and endpoints, retention and investigation tools. The final day turns lab work into an Information Protection and DLP Design mapped to the organisation's classification and privacy duties.
